Figure 3 9/14

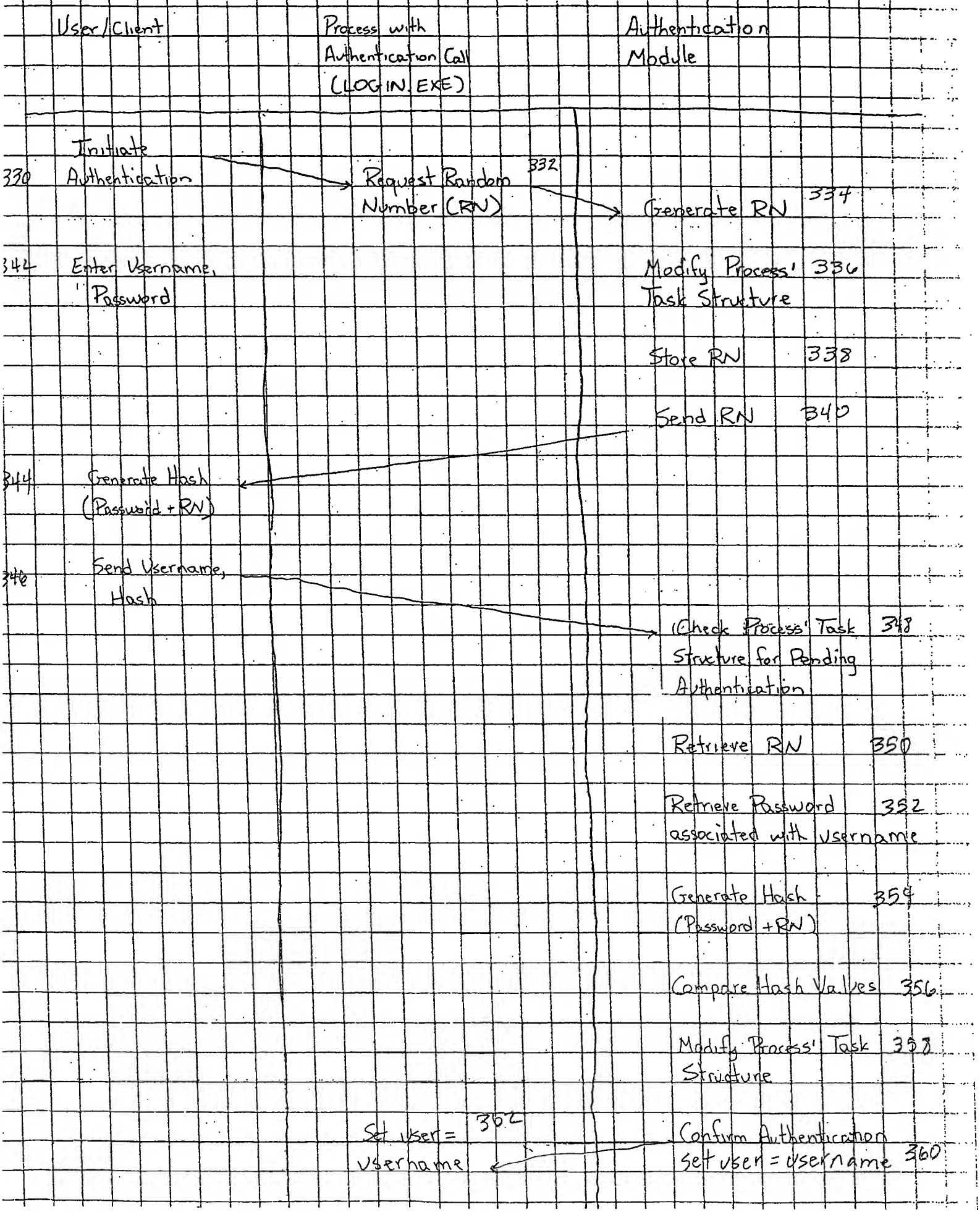

User/Client
Process with Authentication Call (LOGIN.EXE)
Authentication Module
330 Initiate Authentication
332 Request Random Number (RN)
334 Generate RN
344 Enter Username, Password
336 Modify Process' Task Structure
338 Store RN
340 Send RN
344 Generate Hash (Password + RN)
346 Send Username, Hash
348 Check Process' Task Structure for Pending Authentication
350 Retrieve RN
352 Retrieve Password associated with username
354 Generate Hash (Password + RN)
356 Compare Hash Values
358 Modify Process' Task Structure
360 Confirm Authentication set user = username
362 Set user = username

Figure 14

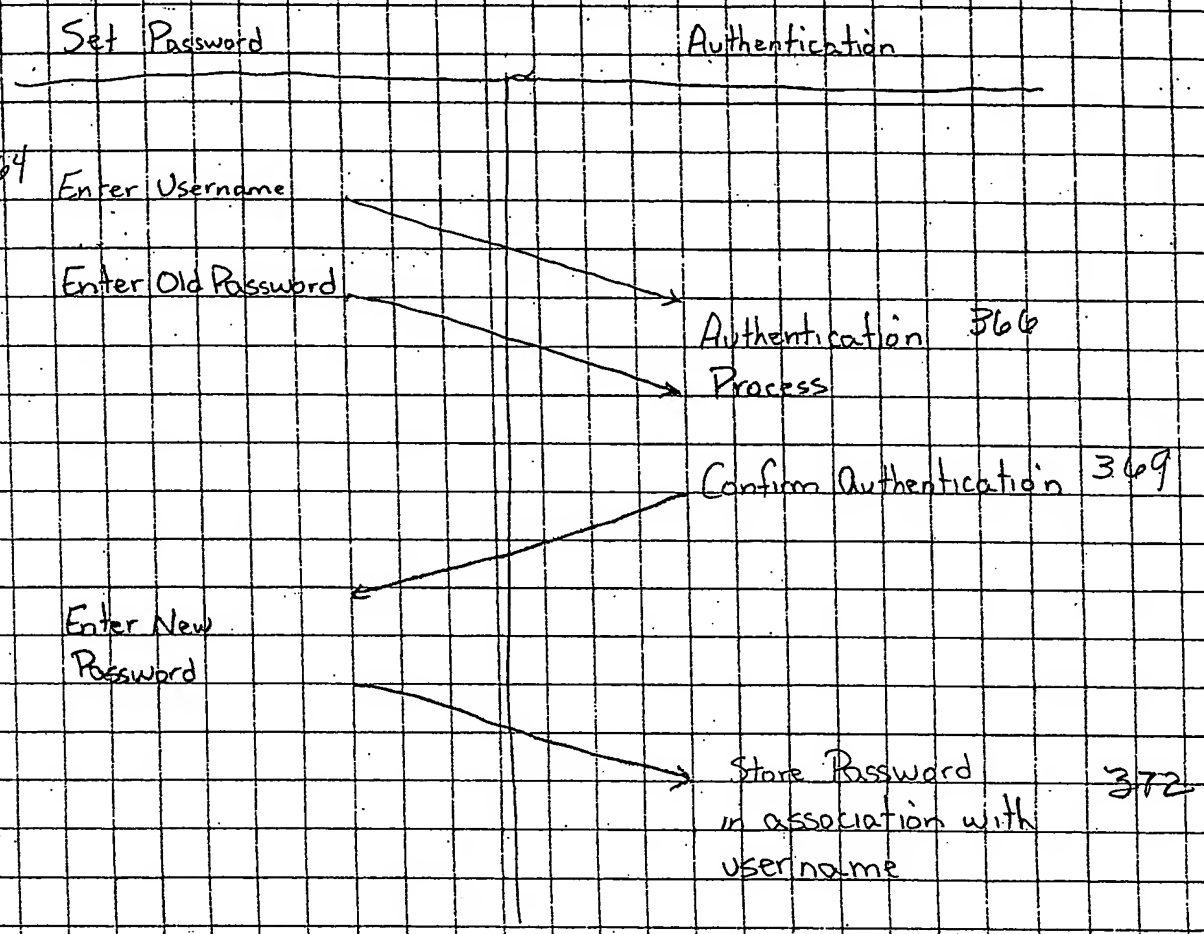

Set Password
Authentication
364
Enter Username
368
Enter Old Password
Authentication Process 366
Confirm Authentication 369
370
Enter New Password
Store Password in association with username 372

Fig. 15

Key Exchange

Client		Server	
374	Request Key Exchange		
375	Send Username		
377	Enter Password (PW)		
		Modify Task Structure	376
		Generate RN1	378
		Send RN1	380
		Retrieve Password (PW) associated with username	382
382	Calculate hash H(PW, RN1)		
		calculate hash H(PW, RN1)	384
386	Key 1 = H(PW, RN1)	Key 1 = H(PW, RN1)	388
		Generate RN2	390
		Send RN2	392
394	calculate hash H(PW, RN2)	calculate hash H(PW, RN2)	396
400	Key 2 = H(PW, RN2)	Key 2 = H(PW, RN2)	398
		Modify Task Structure	402

12/14

Fig 16

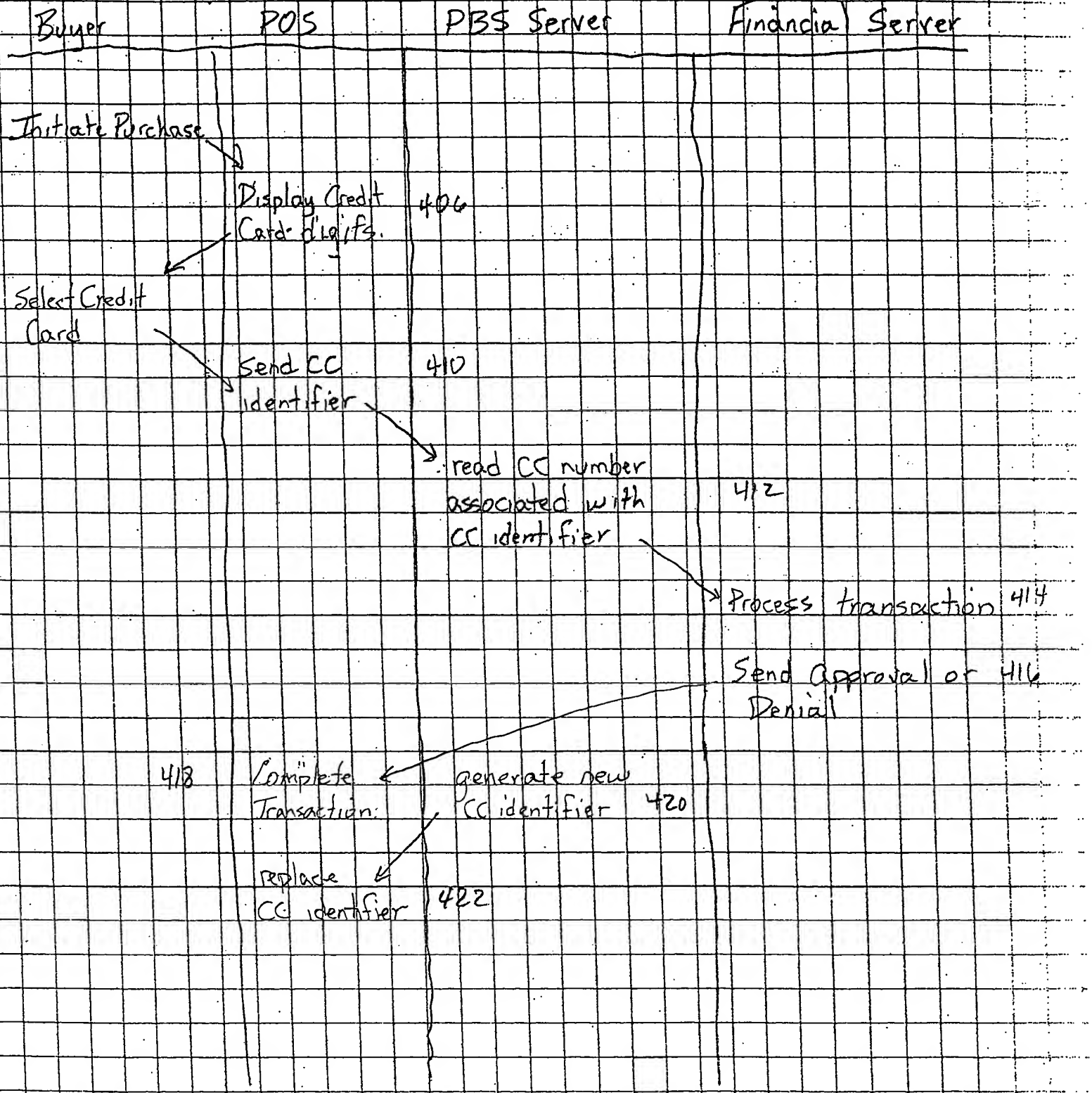
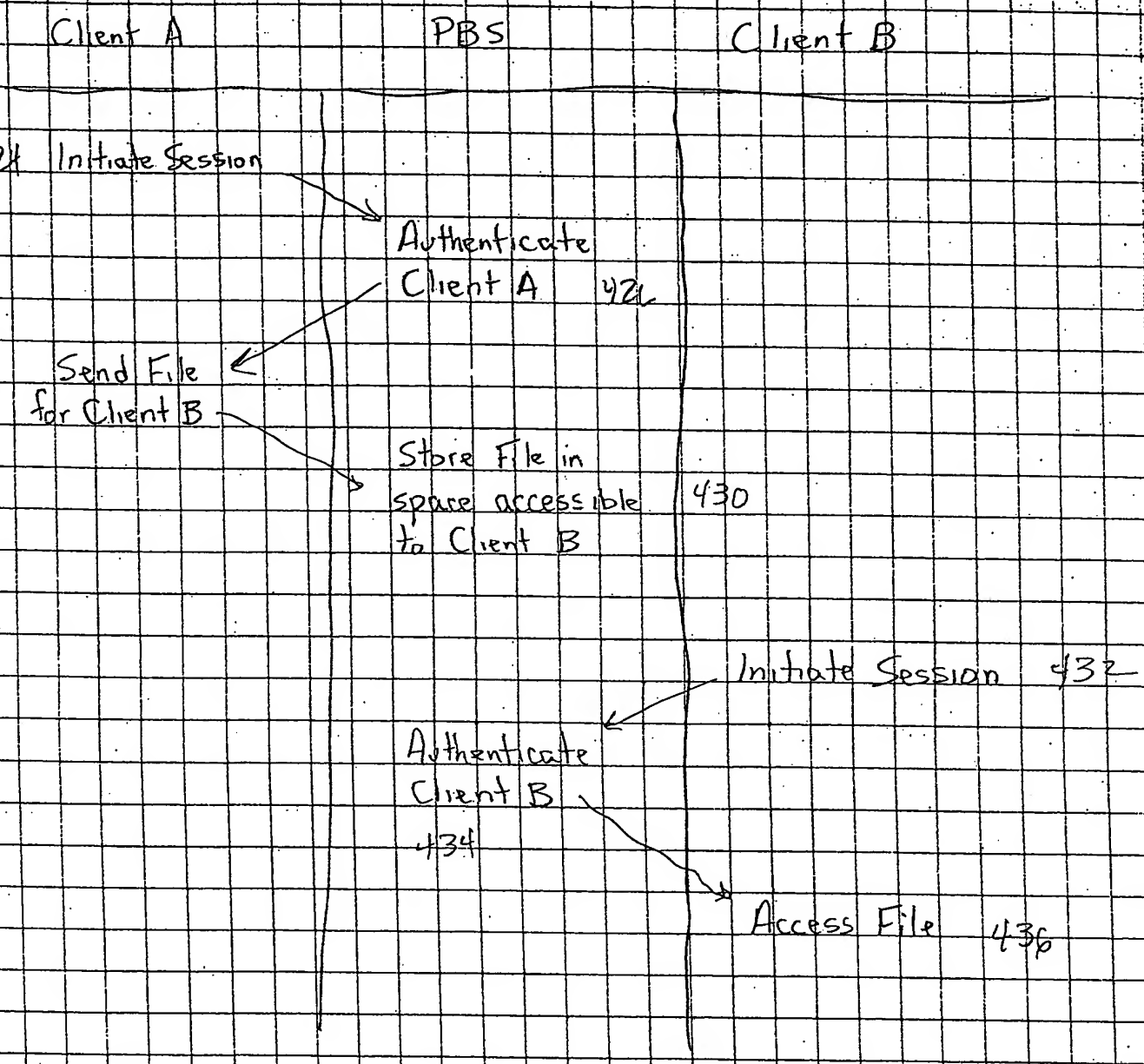

Buyer
POS
PBS Server
Financial Server
Initiate Purchase
Display Credit Card digits.
406
Select Credit Card
Send CC identifier
410
read CC number associated with CC identifier
412
Process transaction
414
Send Approval or Denial
416
418
Complete Transaction
generate new CC identifier
420
replace CC identifier
422

Fig 17


Client A
PBS
Client B
424 Initiate Session
Authenticate Client A 426
428 Send File for Client B
Store File in space accessible to Client B 430
Initiate Session 432
Authenticate Client B 434
Access File 436

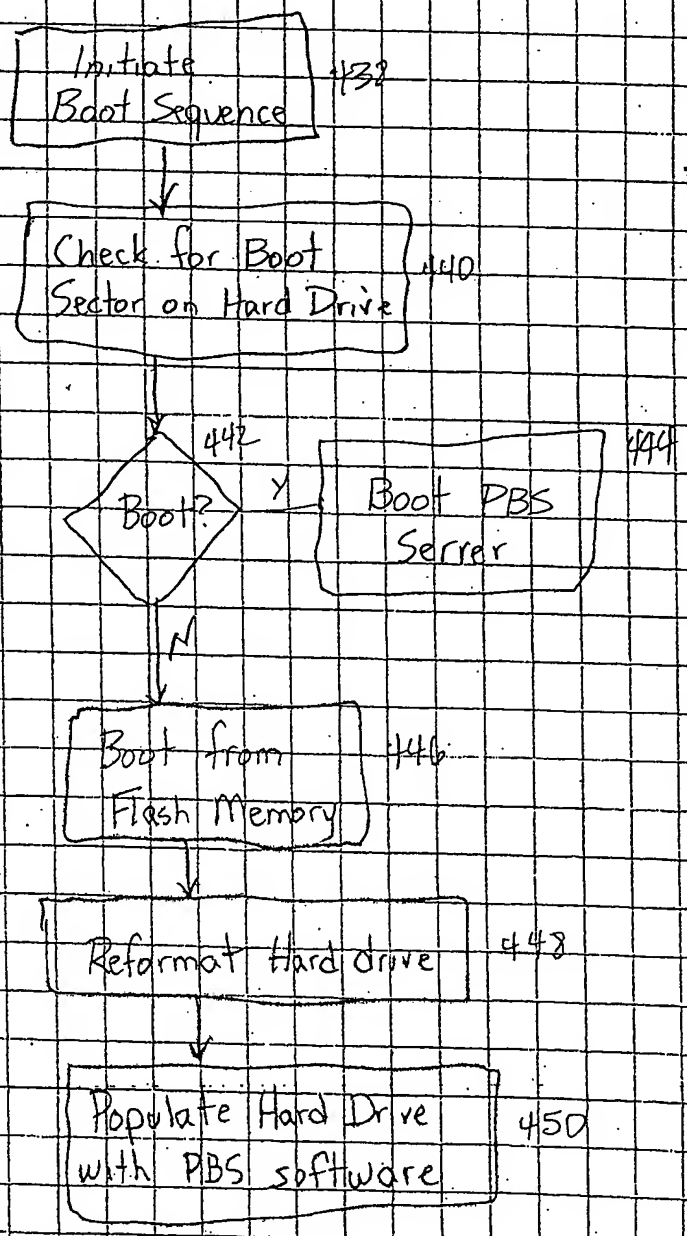

Initiate Boot Sequence
432
Check for Boot Sector on Hard Drive
440
442
Boot?
Y
Boot PBS Server
444
N
Boot from Flash Memory
446
Reformat Hard drive
448
Populate Hard Drive with PBS software
450

Fig 18

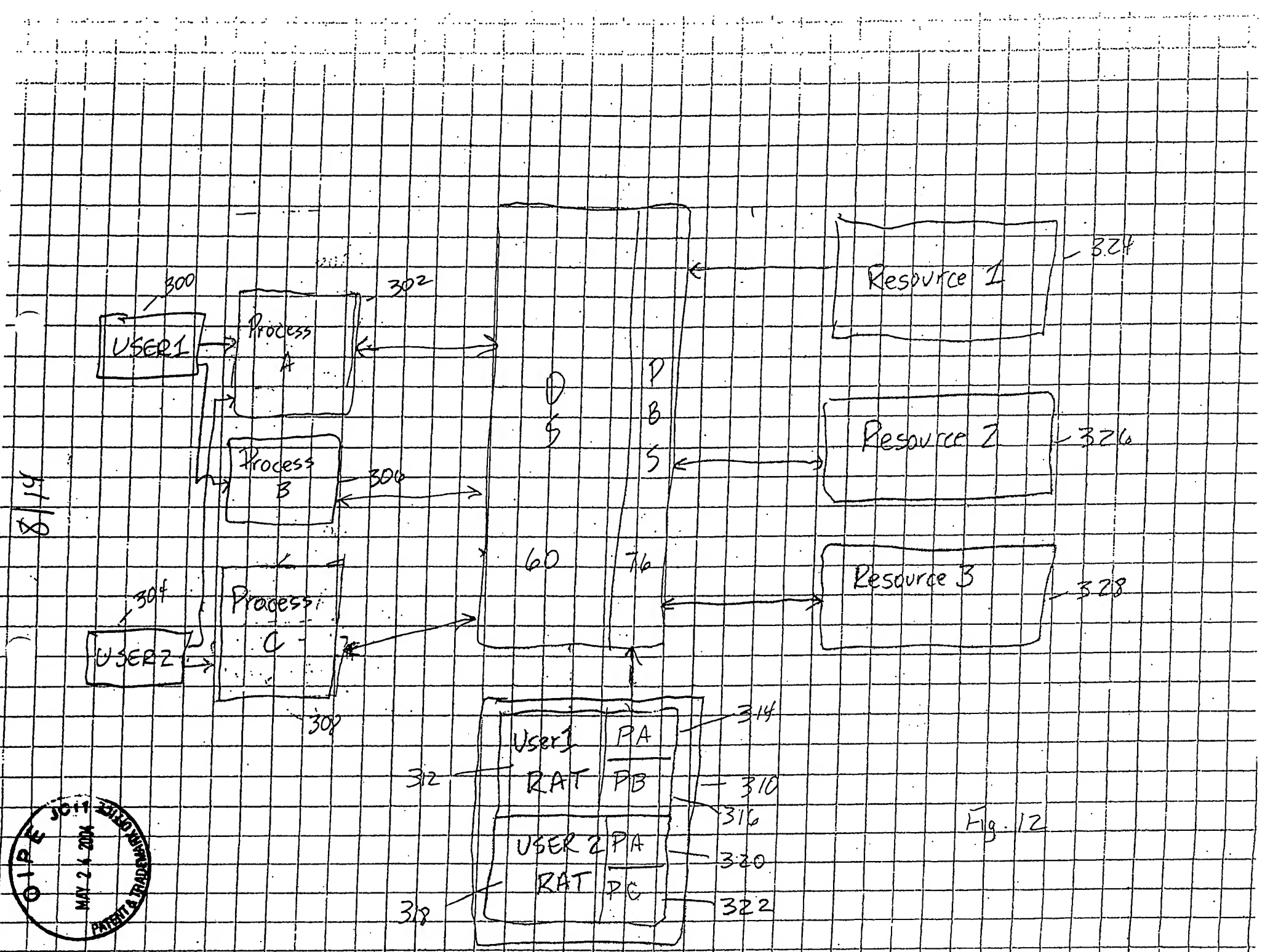


Fig. 12

OIPE JC11 MAY 24 2004 PATENT & TRADEMARK OFFICE